Karlsruhe Institute of Technology

RUB

Horst Görtz Institut für IT-Sicherheit

Polynomial Spaces: A New Framework for Composite-to-Prime-Order Transformations

Crypto 2014, 08-18-2014

Gottfried Herold, Julia Hesse, Dennis Hofheinz, Carla Ráfols, Andy Rupp

Outline

Outline

Outline

Composite-Order Groups

Consider a group

$$\mathbb{G}_N \cong \mathbb{G}_p \times \mathbb{G}_q$$

$$a = (a_p , a_q)$$

put message here!

put randomness there!

Useful feature of $\mathbb{G}_N$: projecting maps

$$\pi : \mathbb{G}_N \longrightarrow \mathbb{G}_N, \quad \pi(\mathbb{G}_q) = \{0\}$$

$$\pi(a) = \pi(a_p, a_q) = (a_p, 0)$$

recover message!

Composite-Order Groups

Consider a group

$$\mathbb{G}_N \cong \mathbb{G}_p \times \mathbb{G}_q$$

$$a = (a_p \ , \ a_q)$$

put message here!

put randomness there!

Useful feature of $\mathbb{G}_N$: projecting maps

$$\pi : \mathbb{G}_N \longrightarrow \mathbb{G}_N, \quad \pi(\mathbb{G}_q) = \{0\}$$

$$\pi(a) = \pi(a_p, a_q) = (a_p, 0)$$

recover message!

Composite-Order Groups

Consider a group

$$\mathbb{G}_N \cong \mathbb{G}_p \times \mathbb{G}_q$$

$$a = (a_p \ , \ a_q)$$

put message here!

put randomness there!

Useful feature of $\mathbb{G}_N$: projecting maps

$$\pi : \mathbb{G}_N \longrightarrow \mathbb{G}_N, \quad \pi(\mathbb{G}_q) = \{0\}$$

$$\pi(a) = \pi(a_p, a_q) = (a_p, 0)$$

recover message!

Composite-Order Groups

Consider a group

$$\mathbb{G}_N \cong \mathbb{G}_p \times \mathbb{G}_q$$

$$a = (a_p \ , \ a_q)$$

put message here!

put randomness there!

Useful feature of $\mathbb{G}_N$: projecting maps

$$\pi : \mathbb{G}_N \longrightarrow \mathbb{G}_N, \quad \pi(\mathbb{G}_q) = \{0\}$$

$$\pi(a) = \pi(a_p, a_q) = (a_p, 0)$$

recover message!

Composite-Order Groups

Consider a group

$$\mathbb{G}_N \cong \mathbb{G}_p \times \mathbb{G}_q$$

$$a = (a_p \ , \ a_q)$$

put message here!

put randomness there!

Useful feature of $\mathbb{G}_N$: projecting maps

$$\pi : \mathbb{G}_N \longrightarrow \mathbb{G}_N, \quad \pi(\mathbb{G}_q) = \{0\}$$

$$\pi(a) = \pi(a_p, a_q) = (a_p, 0)$$

recover message!

Bilinear Groups of Composite-Order

If $\mathbb{G}_N$ additionally has a symmetric pairing

$$\widetilde{e}\colon \mathbb{G}_N \times \mathbb{G}_N \longrightarrow \mathbb{G}_T$$

we have that $\widetilde{e}$ is compatible with π:

$$\widetilde{e}(\pi(a), \pi(b)) = \pi_T(\widetilde{e}(a, b))$$

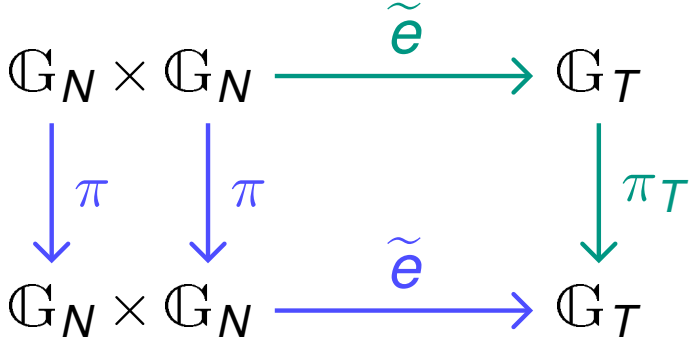
Application: 1-time multiplicatively homomorphic encryption (BGN cryptosystem, where $\widetilde{e}$ is used to multiply encrypted messages)

Bilinear Groups of Composite-Order

If $\mathbb{G}_N$ additionally has a symmetric pairing

$$\widetilde{e}\colon \mathbb{G}_N \times \mathbb{G}_N \longrightarrow \mathbb{G}_T$$

we have that $\widetilde{e}$ is compatible with π:



$$\widetilde{e}(\pi(a), \pi(b)) = \pi_T(\widetilde{e}(a, b))$$

Application: 1-time multiplicatively homomorphic encryption (BGN cryptosystem, where $\widetilde{e}$ is used to multiply encrypted messages)

Security Requirement

$$\underbrace{(0, a_q)}_{\in \mathbb{G}_q = ker(\pi)} \quad \text{or} \quad \underbrace{(1, a_q)}_{\notin \mathbb{G}_q} \; ?$$

Subgroup Indistinguishability (SUB)

$$(\mathbb{G}_N, N, a \xleftarrow{\$} \mathbb{G}_q) \approx_c (\mathbb{G}_N, N, a \xleftarrow{\$} \mathbb{G}_N)$$

- cannot hold if order q is known
- factoring N needs to be hard!

Security Requirement

$$\underbrace{(0, a_q)}_{\in \mathbb{G}_q = ker(\pi)} \quad \text{or} \quad \underbrace{(1, a_q)}_{\notin \mathbb{G}_q} \; ?$$

Subgroup Indistinguishability (SUB)

$$(\mathbb{G}_N, N, a \xleftarrow{\$} \mathbb{G}_q) \approx_c (\mathbb{G}_N, N, a \xleftarrow{\$} \mathbb{G}_N)$$

- cannot hold if order q is known
- factoring N needs to be hard!

Security Requirement

$$\underbrace{(0, a_q)}_{\in \mathbb{G}_q = ker(\pi)} \quad \text{or} \quad \underbrace{(1, a_q)}_{\notin \mathbb{G}_q} \; ?$$

Subgroup Indistinguishability (SUB)

$$(\mathbb{G}_N, N, a \xleftarrow{\$} \mathbb{G}_q) \approx_c (\mathbb{G}_N, N, a \xleftarrow{\$} \mathbb{G}_N)$$

- cannot hold if order q is known
- factoring N needs to be hard!

Security Requirement

$$\underbrace{(0, a_q)}_{\in \mathbb{G}_q = ker(\pi)} \quad \text{or} \quad \underbrace{(1, a_q)}_{\notin \mathbb{G}_q} \; ?$$

Subgroup Indistinguishability (SUB)

$(\mathbb{G}_N, N, a \xleftarrow{\$} \mathbb{G}_q) \approx_c (\mathbb{G}_N, N, a \xleftarrow{\$} \mathbb{G}_N)$

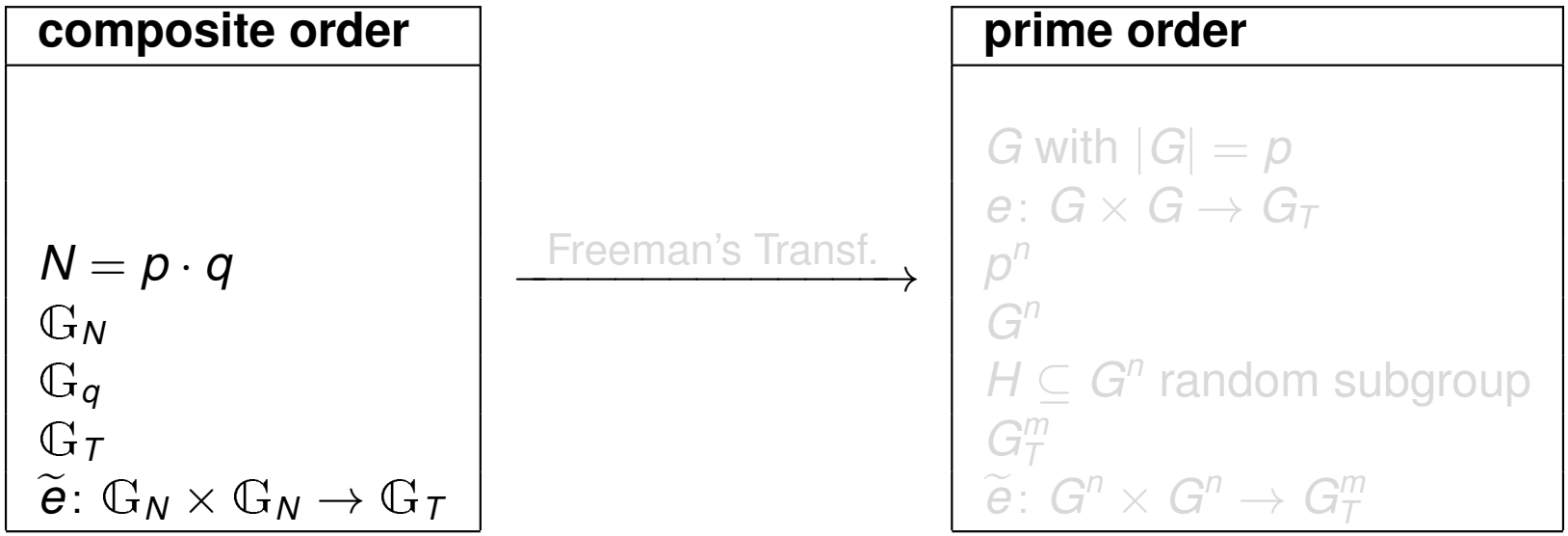
- cannot hold if order q is known
- factoring N needs to be hard!

$\Longrightarrow$ slow pairing evaluation!

Outline

A solution (Freeman, EC'10)

Emulate composite-order groups with prime-order groups:



Identify key properties of the pairing used in the application
Emulate those (projecting / canceling property)

A solution (Freeman, EC'10)

Emulate composite-order groups with prime-order groups:

composite order		prime order
$N = p \cdot q$	Freeman's Transf. $\longrightarrow$	G with $\lvert G \rvert = p$
$\mathbb{G}_N$		$e\colon G \times G \to G_T$
$\mathbb{G}_q$		p^n
$\mathbb{G}_T$		G^n
$\widetilde{e}\colon \mathbb{G}_N \times \mathbb{G}_N \to \mathbb{G}_T$		$H \subseteq G^n$ random subgroup
		G_T^m
		$\widetilde{e}\colon G^n \times G^n \to G_T^m$

Identify key properties of the pairing used in the application
Emulate those (projecting / canceling property)

A solution (Freeman, EC'10)

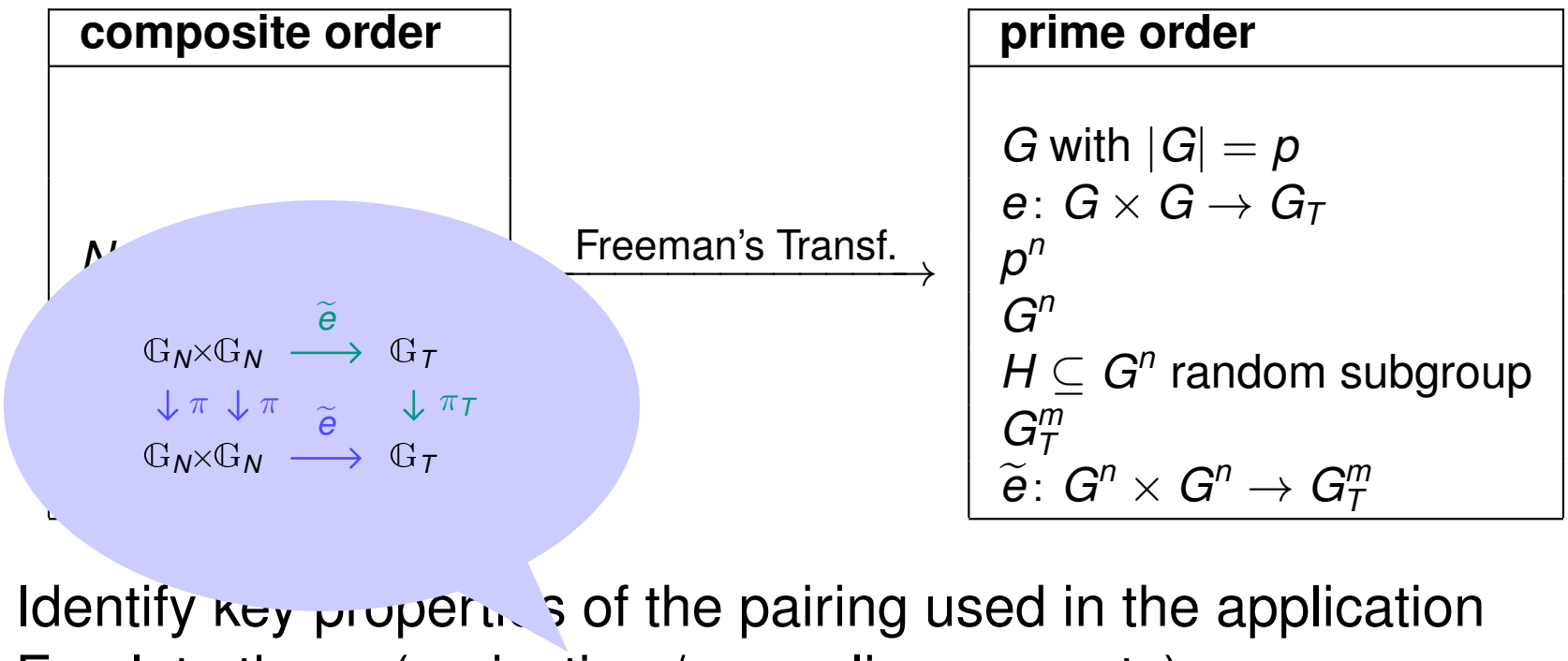
Emulate composite-order groups with prime-order groups:

composite order		**prime order**
$N = p \cdot q$	$\xrightarrow{\text{Freeman's Transf.}}$	G with $\lvert G\rvert = p$
$\mathbb{G}_N$		$e\colon G \times G \to G_T$
$\mathbb{G}_q$		p^n
$\mathbb{G}_T$		G^n
$\widetilde{e}\colon \mathbb{G}_N \times \mathbb{G}_N \to \mathbb{G}_T$		$H \subseteq G^n$ random subgroup
		G_T^m
		$\widetilde{e}\colon G^n \times G^n \to G_T^m$

Identify key properties of the pairing used in the application
Emulate those (projecting / canceling property)

A solution (Freeman, EC'10)

Emulate composite-order groups with prime-order groups:



Identify key properties of the pairing used in the application
Emulate those (projecting / canceling property)

Some notation...

Bracket Notation

$[a]_{\mathcal{P}} := a\mathcal{P}$, but we usually drop the subscript if the basis is $\mathcal{P}$

$[a+b] = [a] + [b]$ ✓ $[ab]_T = e([a],[b])$ ✓ $[ab]$ ✗ $[abc]_T$ ✗

A solution (Freeman, EC'10)

Emulate composite-order groups with prime-order groups:

composite order		**prime order**
$N = p \cdot q$	$\xrightarrow{\text{Freeman's Transf.}}$	G with $\lvert G\rvert = p$
$\mathbb{G}_N$		$e\colon G \times G \to G_T$
$\mathbb{G}_q$		p^n
$\mathbb{G}_T$		G^n
$\widetilde{e}\colon \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$		$H \subseteq G^n$ random subgroup
		G_T^m
		$\widetilde{e}\colon G^n \times G^n \to G_T^m$

A solution (Freeman, EC'10)

Freeman's projecting pairing $\widetilde{e}$

$$\widetilde{e}\left(\begin{pmatrix}[a_0]\\[a_1]\\[a_2]\end{pmatrix},\begin{pmatrix}[b_0]\\[b_1]\\[b_2]\end{pmatrix}\right) = \underbrace{\begin{matrix}([a_0b_0]_T, & [a_0b_1]_T, & \overbrace{[a_0b_2]_T}^{e([a_0],[b_2])},\\ [a_1b_0]_T, & [a_1b_1]_T, & [a_1b_2]_T,\\ [a_2b_0]_T, & [a_2b_1]_T, & [a_2b_2]_T)\end{matrix}}_{\hat{=}\ \begin{pmatrix}a_0 & a_1 & a_2\end{pmatrix}\cdot\begin{pmatrix}b_0\\b_1\\b_2\end{pmatrix}}$$

A solution (Freeman, EC'10)

Emulate composite-order groups with prime-order groups:

composite order		**prime order**
$N = p \cdot q$		G with $\lvert G \rvert = p$
$\mathbb{G}_N$		$e\colon G \times G \to G_T$
$\mathbb{G}_q$	Freeman's Transf. $\longrightarrow$	p^n
$\mathbb{G}_T$		G^n
$\widetilde{e}\colon \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$		$H \subseteq G^n$ **random subgroup**
		G_T^m
		$\widetilde{e}\colon G^n \times G^n \to G_T^m$

A solution (Freeman, EC'10)

Are random subgroups $H \subseteq G^n$ hidden?

This is implied by the Linear Assumption in G.

Such subgroup decision problems are natural:

Observation for $n = 2$

$$\text{DDH hard in } G \Leftrightarrow \text{ SUB hard in } G^2$$

$$([1],[a],[b],[c]) \text{ is a DDH tuple } \Leftrightarrow ([a],[c]) \in \langle([1],[b])\rangle \subseteq G^2$$

A solution (Freeman, EC'10)

Are random subgroups $H \subseteq G^n$ hidden?

This is implied by the Linear Assumption in G.

Such subgroup decision problems are natural:

Observation for $n = 2$

$$\text{DDH hard in } G \Leftrightarrow \text{ SUB hard in } G^2$$

$$([1],[a],[b],[c]) \text{ is a DDH tuple } \Leftrightarrow ([a],[c]) \in \langle([1],[b])\rangle \subseteq G^2$$

A solution (Freeman, EC'10)

Are random subgroups $H \subseteq G^n$ hidden?

This is implied by the Linear Assumption in G.

Such subgroup decision problems are natural:

Observation for $n = 2$

$$\text{DDH hard in } G \Leftrightarrow \text{ SUB hard in } G^2$$

$$([1],[a],[b],[c]) \text{ is a DDH tuple } \Leftrightarrow ([a],[c]) \in \langle([1],[b])\rangle \subseteq G^2$$

A solution (Freeman, EC'10)

Are random subgroups $H \subseteq G^n$ hidden?

This is implied by the Linear Assumption in G.

Such subgroup decision problems are natural:

Observation for $n = 2$

$$\text{DDH hard in } G \Leftrightarrow \text{ SUB hard in } G^2$$

$$([1],[a],[b],[c]) \text{ is a DDH tuple } \Leftrightarrow ([a],[c]) \in \langle([1],[b])\rangle \subseteq G^2$$

Our Results

A framework for emulating composite-order groups that

- provides even **faster pairing computation**
- supports **various security assumptions**
- supports **multilinear** maps
- features **simultaneously projecting & canceling** maps

Our Results

A framework for emulating composite-order groups that

- provides even **faster pairing computation**
- supports **various security assumptions**
- supports **multilinear** maps
- features **simultaneously projecting & canceling** maps

Outline

Our Idea: A Polynomial Viewpoint

Starting like Freeman with copies of prime-order group G

$$G^3 = \begin{pmatrix} G \\ G \\ G \end{pmatrix}$$

. . . but with different interpretation of group elements

$$[\vec{a}] = \begin{pmatrix} [a_0] \\ [a_1] \\ [a_2] \end{pmatrix} \quad \hat{=} \quad a_0 + a_1 X + a_2 X^2 \in \mathbb{Z}_p[X]$$

$\Longrightarrow$ G^3 is $\mathbb{Z}_p$-vector space with basis $\{1, X, X^2\}$.

Our Idea: A Polynomial Viewpoint

Starting like Freeman with copies of prime-order group G

$$G^3 = \begin{pmatrix} G \\ G \\ G \end{pmatrix}$$

. . . but with different interpretation of group elements

$$[\vec{a}] = \begin{pmatrix} [a_0] \\ [a_1] \\ [a_2] \end{pmatrix} \quad \hat{=} \quad a_0 + a_1 X + a_2 X^2 \in \mathbb{Z}_p[X]$$

$\Longrightarrow$ G^3 is $\mathbb{Z}_p$-vector space with basis $\{1, X, X^2\}$.

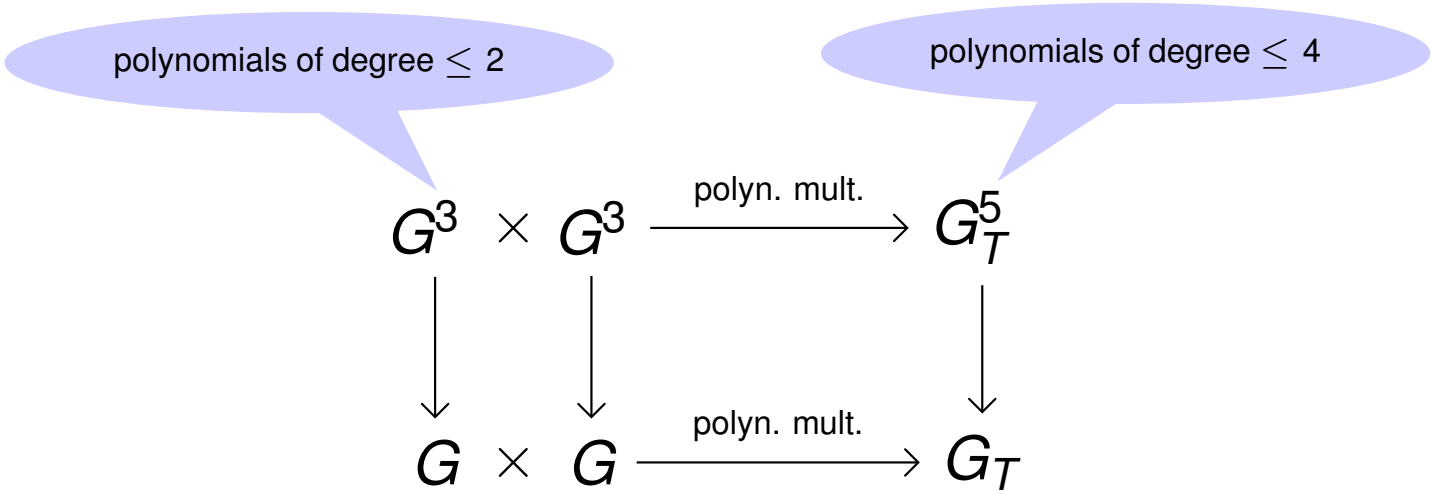
Pairing: Polynomial Multiplication

. . . and polynomial multiplication as pairing $\widetilde{e} : \overbrace{G^3}^{\text{polynomials of degree } \leq 2} \times G^3 \to \underbrace{G_T^5}_{\text{degree } \leq 4}$

$$\widetilde{e}([\vec{a}], [\vec{b}]) = \begin{pmatrix} [a_0 b_0]_T \\ [a_0 b_1]_T + [a_1 b_0]_T \\ [a_0 b_2]_T + [a_1 b_1]_T + [a_2 b_0]_T \\ [a_1 b_2]_T + [a_2 b_1]_T \\ [a_2 b_2]_T \end{pmatrix}$$

computable with evaluations of $e : G \times G \to G_T$

Projections

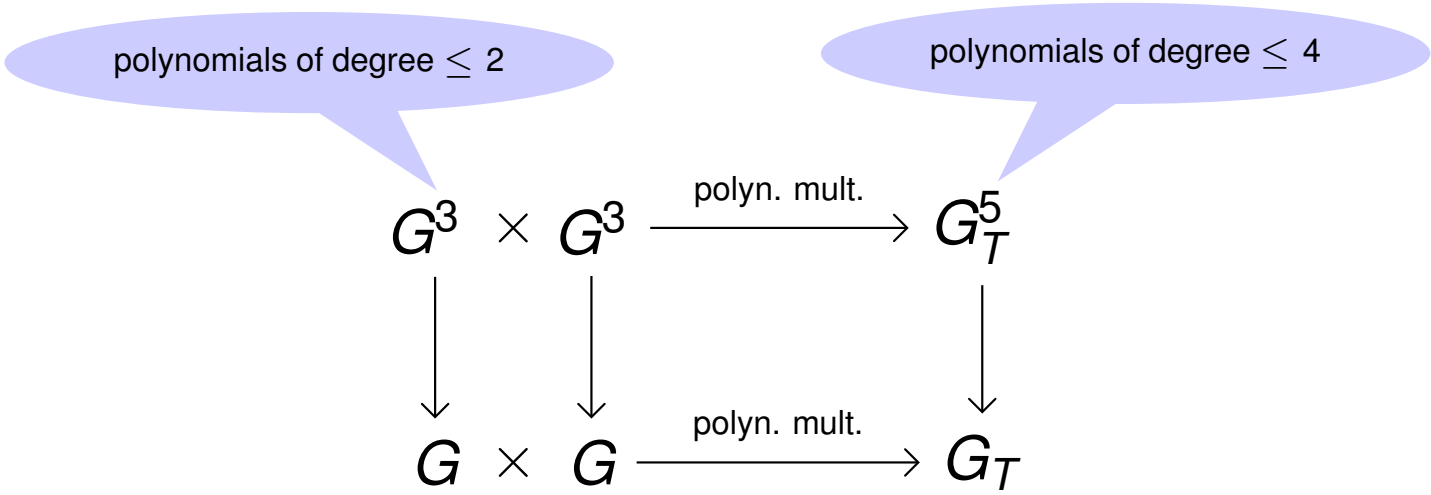


For polynomials $f, g \in \mathbb{Z}_p[X]$ and $s \in \mathbb{Z}_p$ we have

$$f(s) \cdot g(s) = (f \cdot g)(s)$$

$\Longrightarrow$ evaluation is a projection compatible with multiplication!

Projections

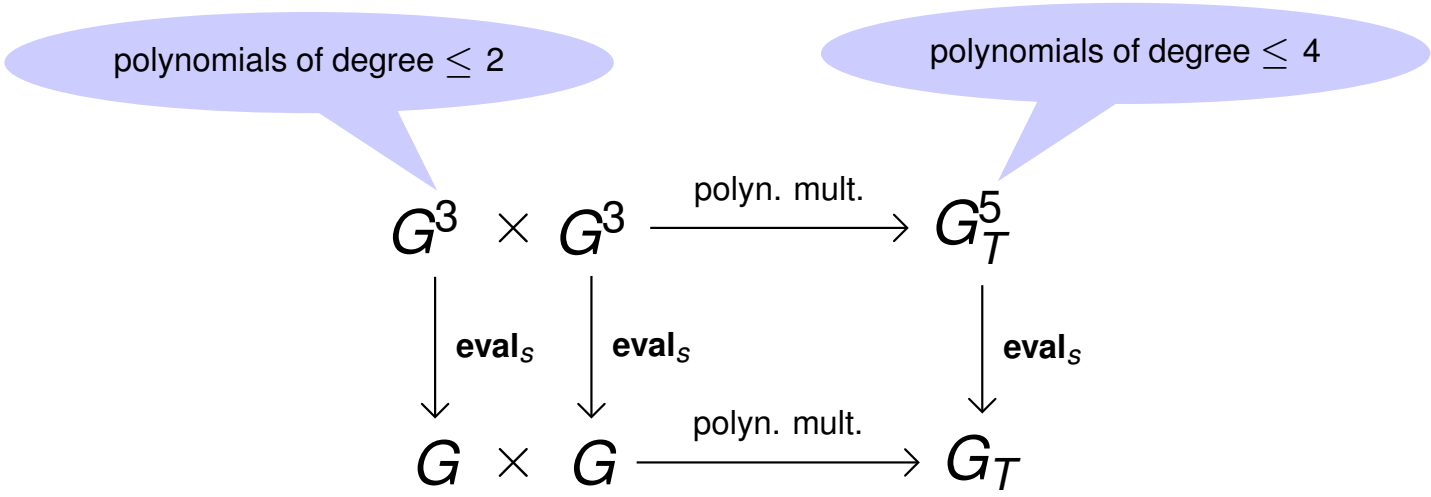


For polynomials $f, g \in \mathbb{Z}_p[X]$ and $s \in \mathbb{Z}_p$ we have

$$f(s) \cdot g(s) = (f \cdot g)(s)$$

$\Longrightarrow$ evaluation is a projection compatible with multiplication!

Projections



For polynomials $f, g \in \mathbb{Z}_p[X]$ and $s \in \mathbb{Z}_p$ we have

$$f(s) \cdot g(s) = (f \cdot g)(s)$$

$\Longrightarrow$ evaluation is a projection compatible with multiplication!

Subgroups

The kernel of $\mathbf{eval}_s$ is

$$\mathbb{H}^s = \{[\vec{a}] \mid a_0 + a_1 s + a_2 s^2 = 0\}$$

A basis for our subgroups:

$$\mathbb{H}^s = \langle \underbrace{\begin{pmatrix} [-s] \\ [1] \\ [0] \end{pmatrix}}_{X-s}, \underbrace{\begin{pmatrix} [0] \\ [-s] \\ [1] \end{pmatrix}}_{X^2-sX} \rangle$$

Is $\mathbb{H}^s$ hidden?

$$[\vec{a}] \in \mathbb{H}^s \iff \vec{a} \in \mathrm{Im}(\mathbf{A}) \text{ with } \mathbf{A} := \begin{pmatrix} -s & 0 \\ 1 & -s \\ 0 & 1 \end{pmatrix}$$

The 2-SCasc Assumption

$$([\mathbf{A}], [\mathbf{A}\vec{w}]) \approx_c ([\mathbf{A}], [\vec{u}])$$

where $\vec{w} \xleftarrow{\$} \mathbb{Z}_p^2$, $\vec{u} \xleftarrow{\$} \mathbb{Z}_p^3$ and $\mathbf{A} := \begin{pmatrix} -s & 0 \\ 1 & -s \\ 0 & 1 \end{pmatrix}$

Thus, our subgroups are hidden if 2-SCasc is hard in G.

Is $\mathbb{H}^s$ hidden?

$$[\vec{a}] \in \mathbb{H}^s \iff \vec{a} \in \mathrm{Im}(\mathbf{A}) \text{ with } \mathbf{A} := \begin{pmatrix} -s & 0 \\ 1 & -s \\ 0 & 1 \end{pmatrix}$$

The 2-SCasc Assumption

$([\mathbf{A}], [\mathbf{A}\vec{w}]) \approx_c ([\mathbf{A}], [\vec{u}])$

where $\vec{w} \xleftarrow{\$} \mathbb{Z}_p^2$, $\vec{u} \xleftarrow{\$} \mathbb{Z}_p^3$ and $\mathbf{A} := \begin{pmatrix} -s & 0 \\ 1 & -s \\ 0 & 1 \end{pmatrix}$

Thus, our subgroups are hidden if 2-SCasc is hard in G.

Is $\mathbb{H}^s$ hidden?

$$[\vec{a}] \in \mathbb{H}^s \iff \vec{a} \in \mathrm{Im}(\mathbf{A}) \text{ with } \mathbf{A} := \begin{pmatrix} -s & 0 \\ 1 & -s \\ 0 & 1 \end{pmatrix}$$

The 2-SCasc Assumption

$([\mathbf{A}], [\mathbf{A}\vec{w}]) \approx_c ([\mathbf{A}], [\vec{u}])$

where $\vec{w} \xleftarrow{\$} \mathbb{Z}_p^2$, $\vec{u} \xleftarrow{\$} \mathbb{Z}_p^3$ and $\mathbf{A} := \begin{pmatrix} -s & 0 \\ 1 & -s \\ 0 & 1 \end{pmatrix}$

Thus, our subgroups are hidden if 2-SCasc is hard in G.

Comparison with Freeman's pairing

$$\widetilde{e}([\vec{a}], [\vec{b}]) =$$

Freeman's Pairing	Our Pairing
$([a_0b_0]_T, [a_0b_1]_T, [a_0b_2]_T,$ $[a_1b_0]_T, [a_1b_1]_T, [a_1b_2]_T,$ $[a_2b_0]_T, [a_2b_1]_T, [a_2b_2]_T)$	$\begin{pmatrix} [a_0b_0]_T \\ [a_0b_1]_T + [a_1b_0]_T \\ [a_0b_2]_T + [a_1b_1]_T + [a_2b_0]_T \\ [a_1b_2]_T + [a_2b_1]_T \\ [a_2b_2]_T \end{pmatrix}$
Uniform Subgroup	Structured Subgroup (SCasc)

Comparison with Freeman's pairing

$$\widetilde{e}([\vec{a}], [\vec{b}]) =$$

Freeman's Pairing

$$\begin{matrix} ([a_0 b_0]_T, & [a_0 b_1]_T, & [a_0 b_2]_T, \\ [a_1 b_0]_T, & [a_1 b_1]_T, & [a_1 b_2]_T, \\ [a_2 b_0]_T, & [a_2 b_1]_T, & [a_2 b_2]_T) \end{matrix}$$

Uniform Subgroup

Our Pairing

$$\begin{pmatrix} [a_0 b_0]_T \\ [a_0 b_1]_T + [a_1 b_0]_T \\ [a_0 b_2]_T + [a_1 b_1]_T + [a_2 b_0]_T \\ [a_1 b_2]_T + [a_2 b_1]_T \\ [a_2 b_2]_T \end{pmatrix}$$

Structured Subgroup (SCasc)

Comparison with Freeman's pairing

$$\widetilde{e}([\vec{a}],[\vec{b}]) =$$

Freeman's Pairing

$$\begin{array}{lll} ([a_0b_0]_T, & [a_0b_1]_T, & [a_0b_2]_T, \\ [a_1b_0]_T, & [a_1b_1]_T, & [a_1b_2]_T, \\ [a_2b_0]_T, & [a_2b_1]_T, & [a_2b_2]_T) \end{array}$$

Uniform Subgroup

Our Pairing

$$\begin{pmatrix} [a_0b_0]_T \\ [a_0b_1]_T + [a_1b_0]_T \\ [a_0b_2]_T + [a_1b_1]_T + [a_2b_0]_T \\ [a_1b_2]_T + [a_2b_1]_T \\ [a_2b_2]_T \end{pmatrix}$$

Structured Subgroup (SCasc)

Efficiency improvements

How to Multiply Polynomials

$$\widetilde{e}([\vec{a}],[\vec{b}]) = \begin{pmatrix} [a_0 b_0]_T \\ [a_0 b_1]_T + [a_1 b_0]_T \\ [a_0 b_2]_T + [a_1 b_1]_T + [a_2 b_0]_T \\ [a_1 b_2]_T + [a_2 b_1]_T \\ [a_2 b_2]_T \end{pmatrix}$$

- Schoolbook multiplication: 9 applications of e
- Fast polynomial multiplication: 5 applications of e

Efficiency improvements

How to Multiply Polynomials

$$\widetilde{e}([\vec{a}],[\vec{b}]) = \begin{pmatrix} [a_0 b_0]_T \\ [a_0 b_1]_T + [a_1 b_0]_T \\ [a_0 b_2]_T + [a_1 b_1]_T + [a_2 b_0]_T \\ [a_1 b_2]_T + [a_2 b_1]_T \\ [a_2 b_2]_T \end{pmatrix}$$

- Schoolbook multiplication: 9 applications of e
- Fast polynomial multiplication: 5 applications of e

Generalizations

- Generalizes naturally to k-linear maps
- Generalizes to other matrix assumptions
  (e.g. k-LIN or a uniform choice of subgroup)
- Optimal size of image for any matrix assumption
- Fast polynomial multiplication is still possible
  Number of applications of e = dimension of image

Outline

Efficiency Comparison

Construction	Ass.	Domain	Image	Cost $\widetilde{e}$
Freeman, $k = 2$	uniform	3	9	9 e
Seo, $k = 2$	uniform	3	6	9 e + 3 gop
Our work, $k = 2$	uniform	3	6	6 e + 12 mexp
Our work, $k = 2$	2-SCasc	3	5	5 e + 22 gop
Freeman, $k > 2$	uniform	$k+1$	$O(k^k)$	$O(k^k)$ e
Our work, $k > 2$	uniform	$k+1$	$O(2^k)$	$O(2^k)$ e + $O(2^k)$ mexp
Our work $k > 2$	k-SCasc	$k+1$	$O(k^2)$	$O(k^2)$ e + $O(k^3)$ mexp

e = prime-order pairing
mexp= multiexponentiation
gop = group operation

Efficiency Comparison

Construction	Ass.	Domain	Image	Cost $\widetilde{e}$
Freeman, $k = 2$	uniform	3	9	9 e
Seo, $k = 2$	uniform	3	6	9 e + 3 gop
Our work, $k = 2$	uniform	3	6	6 e + 12 mexp
Our work, $k = 2$	2-SCasc	3	5	5 e + 22 gop
Freeman, $k > 2$	uniform	$k+1$	$O(k^k)$	$O(k^k)$ e
Our work, $k > 2$	uniform	$k+1$	$O(2^k)$	$O(2^k)$ e + $O(2^k)$ mexp
Our work $k > 2$	k-SCasc	$k+1$	$O(k^2)$	$O(k^2)$ e + $O(k^3)$ mexp

e = prime-order pairing
mexp= multiexponentiation
gop = group operation

Outline

Summary

Modification of Freeman's Framework:

- polynomial multiplication as bilinear map
- structured subgroups instead of random ones
- security from any matrix assumption

Many benefits:

- Faster composite-order GS proofs (save about half of the pairings)
- Faster composite-order cryptosystems (BGN, predicate encryption etc.)

Summary

Modification of Freeman's Framework:

- polynomial multiplication as bilinear map
- structured subgroups instead of random ones
- security from any matrix assumption

Many benefits:

- Faster composite-order GS proofs (save about half of the pairings)
- Faster composite-order cryptosystems (BGN, predicate encryption etc.)

Summary

Modification of Freeman's Framework:

- polynomial multiplication as bilinear map
- structured subgroups instead of random ones
- security from any matrix assumption

Many benefits:

- Faster composite-order GS proofs (save about half of the pairings)
- Faster composite-order cryptosystems (BGN, predicate encryption etc.)

Thank you for your attention!

References

- D. M. Freeman, “Converting pairing-based cryptosystems from composite-order groups to prime-order groups,” 2010, pp. 44–61.
- J. H. Seo, “On the (im)possibility of projecting property in prime-order setting,” 2012, pp. 61–79.
- A. Escala, G. Herold, E. Kiltz, C. Ràfols, and J. Villar, “An algebraic framework for Diffie-Hellman assumptions,” 2013, pp. 129–147.